DNSFilter

DNS Protection for In-Flight Connectivity

Every aircraft is a flying public Wi-Fi hotspot. DNSFilter protects it.

The Problem

Free Wi-Fi is now standard. American, Delta, and United are rolling it out fleet-wide in 2026. That's 150-400 devices per aircraft on a shared, unfiltered network.

600
PERCENT
year-over-year increase in aviation cyber attacks.

7
YEARS
prison sentence for Australian man found guilty of evil twin attacks.

6
MILLION
customer records exposed in Quantas attack.

$200-250
MILLION
annual spending per airline on in-flight connectivity

MANDATES
TSA cybersecurity directives now mandate network monitoring and access controls

What DNSFilter Does

Provider-agnostic DNS filtering for in-flight connectivity. Works across Starlink, Viasat, Panasonic, Kuiper. Switch ISPs without reconfiguring security.

No hardware on aircraft.
Operates at the network DNS level. Zero impact on weight, fuel, or maintenance.

Captive portal compatible.
Travel Wi-Fi Mode keeps airline login portals working while filtering stays active. Competitors break here.

AI threat detection.
We process 200B+ queries daily and block malicious domains 10 days before traditional threat feeds.

Content filtering.
Limit bandwidth-heavy streaming, enforce acceptable use, maintain family-appropriate browsing.

TSA Compliance Mapping

TSA cybersecurity directives require airlines to implement specific controls. DNS filtering maps directly to these requirements.

TSA Requirement	How DNS Filtering Addresses It
Continuous Monitoring	DNS query logs provide real-time visibility into every connection attempt on the network.
Access Controls	DNS filtering restricts access to known-malicious domains and enforces acceptable use policies.
Network Segmentation	DNS policies create a policy-enforced boundary at the DNS layer, separating passenger traffic from operational systems.
Incident Response	DNS logs provide forensic evidence of connection attempts, blocked threats, and policy violations.

DNS query logs and filtering policies give airlines audit-ready compliance evidence for TSA directives, EASA Part IS requirements, and ICAO cybersecurity frameworks.

GET IN TOUCH

🌐 dnsfilter.com/industry/aviation ☎ (877) 331-2412 ✉ sales@dnsfilter.com

Why DNSFilter?

TSA cybersecurity directives require airlines to implement specific controls. DNS filtering maps directly to these requirements.

	DNSFilter	ISP-Level Filtering
All satellite ISPs	Yes	Tied to one provider
AI threat detection	10 days faster	Basic blocklists
TSA compliance mapping	Direct	Partial
No aircraft hardware	Yes	Depends

DNS query logs and filtering policies give airlines audit-ready compliance evidence for TSA directives, EASA Part IS requirements, and ICAO cybersecurity frameworks.

How It Works

1. **POINT DNS**
Configure IFC network DNS to DNSFilter. No hardware. No aircraft downtime.

2. **SET POLICIES**
Block threats, restrict content, create per-segment policies. Applies across all aircraft and ISPs.

3. **MONITOR**
Real-time dashboards. Fleet-wide visibility. Export logs for TSA audits.

By The Numbers

- **453,000+** organizations protected
- **200B+** DNS queries processed daily
- **175M+** threats blocked dail
- **3,100+** MSP partners
- **10 days** faster threat detection than traditional feeds
- Deploys in **minutes,** not months

Cost Perspective

Airlines spend $200-250M/year on IFC infrastructure. DNS filtering costs pennies per passenger per flight. Lowest-cost, highest-impact security layer you can add to any IFC deployment.

Book a demo tailored to your fleet's architecture → https://www.dnsfilter.com/book-a-live-demo

SOC 2 Type II certified.

GET IN TOUCH

dnsfilter.com/industry/aviation

☎ (877) 331-2412

✉ sales@dnsfilter.com